Journal of Algebraic Combinatorics 1 (1992), 347–351

A Graham-Sloane Type Construction for s-Surjective Matrices

IIRO HONKALA
Department of Mathematics, University of Turku, 20500 Turku 50, Finland

Received July 22, 1992

Abstract. We give a construction of $(n-s)$-surjective matrices with n columns over $\mathbb{Z}_q$ using Abelian groups and additive s-bases. In particular we show that the minimum number of rows $ms_q(n, n-s)$ in such a matrix is at most $s^s q^{n-s}$ for all q, n and s.

Keywords: s-surjective matrix, additive basis, orthogonal array.

1. Introduction

We say that an $m \times n$ matrix A over $\mathbb{Z}_q$ is s-surjective if it has the following property: if we choose any s columns $i_1, \cdots, i_s$ and any s-tuple $(a_1, \cdots, a_s)$ of integers modulo q then there is a row of A which has a_j in the column i_j for every $j = 1, \cdots, s$. In this paper we study the question what is the smallest possible number $ms_q(n, s)$ of rows in an s-surjective matrix over $\mathbb{Z}_q$ with n columns. For an application of s-surjective matrices to coding for memories with defects, see [7].

Trivially $ms_q(n, 1) = q$ and it is easy to see that $ms_q(n, n-1) = q^{n-1}$ (take as rows all the $(a_1, \cdots, a_n) \in \mathbb{Z}_q^n$ for which $a_1 + \cdots + a_n = 0$). In general

$$ms_q(n, s) \geq q^s. \tag{1}$$

If equality holds in (1) then there exists a $q^s \times n$ matrix such that every s-tuple of integers modulo q appears exactly once in any given s columns, that is, there exists an orthogonal array of size q^s, n constraints, q levels, strength s and index 1 [17, p. 328]. For $s = 2$ the existence of such an orthogonal array is equivalent to the existence of $n-2$ mutually orthogonal Latin squares of order q; see, e.g., [3, Theorem 5.2.1]. It is known—see [12, Ch. 13] or [3, Ch. 5]—that there are two mutually orthogonal Latin squares of every order $q \neq 2$, 6, and therefore $ms_q(4, 2) = q^2$ for all $q \neq 2$, 6.

If q is a prime power then by [17, p. 329] the rows of a linear orthogonal array A of size q^s, n constraints, q levels, strength s and index 1 (with the elements of A from $GF(q)$) are the codewords of an $[n, s]$ maximum distance separable (MDS) code over $GF(q)$ and conversely. It is known (see [17, p. 327–8]) that there exists an $[n, s]$ MDS code over $GF(q)$ for all $1 \leq s \leq q$ and $n \leq q + 1$.

From number theory we know that for every $\varepsilon > 0$ there is an $n_0(\varepsilon)$ such that for all $n > n_0(\varepsilon)$ there is a prime in the interval $(n, (1+\varepsilon)n)$ [11, p. 88]. These two facts together imply that

$$ms_q(n,s) \sim q^s \text{ for fixed } n \text{ and } s \text{ as } q \to \infty.$$

A trivial upper bound on $ms_q(n,s)$ is

$$ms_q(n,s) \le \binom{n}{s} q^s. \tag{2}$$

Many bounds on $ms_q(n,s)$ can be found in [6], [15] and [19]. It is known that

$$ms_q(n,s) = O(\log(n)) \text{ for fixed } q \text{ and } s \text{ as } n \to \infty,$$

see [15] and [19]. For an explicit construction in the case $q = 2$, see [1]. For a table of lower and upper bounds on $ms_2(n,s)$ for small values of n and s, see [19].

For $q = 2$ the exact values of $ms_q(n,s)$ have also been determined for $s = 2$, see [4], [15] (alternatively see [2, Chapter 5]) and for $s = n-2$ by Roux [19]. For $s = n-2$ the result is

$$ms_2(n, n-2) = \lfloor 2^n/3 \rfloor$$

(for a short proof, see [14, Theorem 6]). More generally, it is shown in [19] that

$$ms_2(n, n-s) \le \sum_{w \in W} \binom{n}{w}, \tag{3}$$

where $W = \{w \mid 0 \le w \le n, w \equiv a (\text{mod } s+1)\}$ for any $a = 0, 1, \cdots, s$ (take all the rows on which the number of l's belongs to W, i.e., all the rows whose *weight* belongs to W).

The purpose of this paper is to consider the function $ms_q(n, n-s)$ for a fixed s, and show in Theorem 1 how (3) can be generalized to this case. In order to do that we generalize the concept of weight in an interesting way by labelling the letters of the alphabet $\mathbb{Z}_q$ by elements of an additive basis in a larger Abelian group. Using Theorem 1 we show in Theorem 4 that

$$ms_q(n, n-s) \le s^s q^{n-s} \text{ for all } q, n, s, \tag{4}$$

which shows that for any fixed s we have

$$ms_q(n, n-s) = O(q^{n-s}) \text{ as } q, n \to \infty$$

where q and n tend to infinity independently of each other. For specific values of s we can often improve on (4), see Corollary 3 and Examples 1 and 2.

In [9] Graham and Sloane give interesting lower bounds for binary constant weight codes, see also [16]. For an excellent survey on constant weight codes, see [5]. Our construction resembles the constructions in [9] and [16], but is in a sense dual to that.

2. A construction using Abelian groups

THEOREM 1. *Assume that G is an additive Abelian group with g elements and $Q \subseteq G$ is a q-element subset of G such that every element of G can be written as a sum of exactly s (not necessarily distinct) elements of Q. Then*

$$ms_q(n, n-s) \leq \frac{1}{g} q^n \text{ for all } n.$$

Proof. Let $r : \mathbb{Z}_q \to Q$ be a bijection. We show that a matrix having as rows the elements of the set

$$C_a = \{(c_1, c_2, \cdots, c_n) \in \mathbb{Z}_q^n \mid r(c_1) + r(c_2) + \cdots + r(c_n) = a\}$$

for any fixed $a \in G$, is $(n-s)$-surjective. We show that for any indices $i_1, \cdots, i_{n-s}$ and any $b_1, \cdots, b_{n-s} \in \mathbb{Z}_q$ there is an element $(c_1, \cdots, c_n) \in C_a$ such that $c_{i_k} = b_k$ for all $k = 1, \cdots, n-s$. W.l.o.g. $i_1 = s+1, i_2 = s+2, \cdots, i_{n-s} = n$. Because every element of G can be represented as a sum of exactly s elements of Q, we can choose $b_1, \cdots, b_s \in \mathbb{Z}_q$ in such a way that

$$r(b_1) + r(b_2) + \cdots + r(b_s) = a - r(b_{s+1}) - \cdots - r(b_n).$$

Then $(b_1, \cdots, b_n) \in C_a$ is as required.

The set $\mathbb{Z}_q^n$ is the union of the g sets $C_a, a \in G$. Hence at least one of the sets C_a contains at most q^n/g elements. □

If h and k are positive integers, an additive h-basis of size k for n is a set $A = \{a_0 = 0, a_1 = 1, a_2, a_3, \cdots, a_k\}$ of integers such that every integer i with $0 \leq i \leq n$ can be expressed as a sum of exactly h (not necessarily distinct) elements of A. The largest integer n for which there exists an h-basis of size k is denoted by $f(h,k)$. The function $f(h,k)$ has been extensively studied (see e.g., Mathematical Reviews, Section 11B13). Any lower bound on $f(h,k)$ can be used in Theorem 1 to obtain upper bounds on $ms_q(n, n-s)$ (we choose $G = \mathbb{Z}_n, n = 1 + f(s, q-1)$, in Theorem 1).

COROLLARY 2. $ms_q(n, n-s) \leq \frac{1}{1+f(s,q-1)} q^n$.

For example, from [13] we obtain the following corollary.

COROLLARY 3. $ms_q(n, n-2) \leq \frac{1}{1+5(q-1)^2/18} q^n \leq \frac{18}{5} \left(\frac{q}{q-1}\right)^2 q^{n-2}$.

Example 1. For $q = 3, 4$ and 5 and $s = 2$, we can choose $Q = \{0,1,3\} \subseteq \mathbb{Z}_5, \{0,1,3,4\} \subseteq Z_9$ and $\{0,1,3,5,6\} \subseteq \mathbb{Z}_{13}$ respectively, to obtain

$$ms_3(n, n-2) \leq \tfrac{9}{5}\, 3^{n-2} \text{ for all } n,$$

$$ms_4(n, n-2) \leq \tfrac{16}{9}\, 4^{n-2} \text{ for all } n,$$

$$ms_5(n, n-2) \leq \tfrac{25}{13}\, 5^{n-2} \text{ for all } n.$$

For specific values of q, n and s the sets $C_a (a \in G)$ in the proof of Theorem 1 can of course be of different sizes. For example, in the case $q = 3$, $s = 2$, $n = 4$, the sets C_0, C_1, C_2, C_3, C_4 have 17, 14, 19, 14 and 17 elements respectively thus yielding the upper bound $ms_3(4, 2) \leq 14$ (the true value is 9 as mentioned in the introduction).

In general, we can take any Abelian group instead of a cyclic group. The following simple theorem shows that, interestingly, for any fixed s there is a constant s^s such that $ms_q(n, n-s) \leq s^s q^{n-s}$ for all q and n where q^{n-s} is the trivial lower bound on $ms_q(n, n-s)$. A similar result can also be proved using cyclic groups and a result of Rohrbach [18]; in fact the proof of Theorem 4 is essentially from [18, pp. 24–25]. From the proof we also see that constructing such matrices is easy for fixed s.

THEOREM 4. $ms_q(n, n-s) \leq s^s q^{n-s}$.

Proof. Suppose $q - 1 = as + b$, where $0 \leq b < s$. We choose in Theorem 1 the group $G = \mathbb{Z}_{a+2}^b \oplus \mathbb{Z}_{a+1}^{s-b}$ and $Q = \{(c_1, c_2, \cdots, c_s) \mid c_i \neq 0 \text{ for at most one } i\}$. Then $|Q| = 1 + b(a+1) + (s-b)a = q$, and every element of G can clearly be written as a sum of exactly s elements of Q. Now $|G| = (a+2)^b (a+1)^{s-b} \geq (a+1)^s = (\lfloor (q-1)/s \rfloor + 1)^s \geq (q/s)^s$ and the result follows from Theorem 1. □

COROLLARY 5. $ms_q(n, n-s) = O(q^{n-s})$ for fixed s as $q, n \to \infty$. □

In Corollary 5 we can assume that $q \to \infty$ and $n \to \infty$ independently of each other. For a fixed value of q, the result of Corollary 5 is trivial because always $ms_q(n, n-s) \leq q^n = q^s \cdot q^{n-s}$; likewise for a fixed n, the result would trivially follow from (2).

In the case $q = 2$ Theorem 1 and its proof give the result 2.6 of [19, p. 25].

If there exists a binary linear code C of length $q-1$ and dimension $q-1-k$ with covering radius s then the columns of the $k \times (q-1)$ parity check matrix of C together with the zero element of $\mathbb{Z}_2^k$ have the property that every element of $\mathbb{Z}_2^k$ can be represented as a sum of exactly s of them (see [8]), and consequently, by Theorem 1 we then have

$$ms_q(n, n-s) \leq \frac{1}{2^k}\, q^n \text{ for all } n.$$

For tables of linear covering codes, see e.g., [10].

Example 2. There exists a binary linear code of length 23, dimension 12 and covering radius 3, and therefore,

$$ms_{24}(n, n-3) \leq \frac{27}{4}\, 24^{n-3} \text{ for all } n,$$

which is much better than the estimate $ms_{24}(n, n-3) \leq 27 \times 24^{n-3}$ of Theorem 4.

Acknowledgment

The author would like to thank the referee for useful remarks.

References

1. N. Alon, "Explicit construction of exponential sized families of k-independent sets," *Discrete Math.*, **56** (1986), 191–193.
2. I. Anderson, *Combinatorics of Finite Sets*, Clarendon Press, Oxford, 1987.
3. I. Anderson, *Combinatorial Designs: Construction Methods*, Ellis Horwood Limited, Chichester, 1990.
4. A. Brace and D. E. Daykin, "Sperner type theorems for finite sets," *Proc. Br. Combinatorial Conf., Oxford* (1972), 18–37, Institute of Mathematics and its Applications, Southend-on-Sea.
5. A.E. Brouwer, J.B. Shearer, N.J.A. Sloane, and W.D. Smith, "A new table of constant weight codes," *IEEE Trans. Inform. Theory*, **36** (1990) 1334–1380.
6. P. Busschbach, "Constructive methods to solve problems of s-surjectivity, conflict resolution, coding in defective memories," Rapport Interne ENST 84D005, Paris, Dec. 1984.
7. G.D. Cohen, "Applications of coding theory to communication combinatorial problems," *Discrete Math.*, **83** (1990) 237–248.
8. G.D. Cohen, M.G. Karpovsky, H.F. Mattson, Jr., and J. R. Schatz, "Covering radius—survey and recent results," *IEEE Trans. Inform. Theory*, **31** (1985) 328–343.
9. R. L. Graham and N.J.A. Sloane, "Lower bounds for constant weight codes," *IEEE Trans. Inform. Theory*, **26** (1980) 37–43.
10. R.L. Graham and N.J.A. Sloane, "On the covering radius of codes," *IEEE Trans. Inform. Theory*, **31** (1985) 385–401.
11. H. Halberstam and K.F. Roth, *Sequences*, vol. 1, Oxford Univ. Press, Oxford, 1966.
12. M. Hall Jr., *Combinatorial Theory*, John Wiley & Sons, New York, 2nd edition, 1986.
13. N. Hämmerer and G. Hofmeister, "Zu einer Vermutung von Rohrbach," *J. Reine Angew. Math.*, **286/287** (1976) 239–247.
14. I. Honkala, "Modified bounds for covering codes," *IEEE Trans. Inform. Theory*, **37** (1991) 351–365.
15. D.J. Kleitman and J. Spencer, "Families of independent sets," *Discrete Math.*, **6** (1973) 255–262.
16. T. Kløve, "A new lower bound for $A(n, 4, w)$," *IEEE Trans. Inform. Theory*, **27** (1981) 257–258.
17. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
18. H. Rohrbach, "Ein Beitrag zur additiven Zahlentheorie," *Math. Zeitschr.*, **42** (1936) 1–30.
19. G. Roux, "k-propriétés des tableaux de n colonnes," Thèse Doctorat Univ. Paris 6, March 1987.